# Information Protection Policy

**2024. 04. 22**

# Document History

| No. | Version | Dafe | Key Points | Drafter | Approver |
|---|---|---|---|---|---|
| 1 | 1.0 | 2024.04.22 | New enactment | LEE, Yun-jae | CEO |
| 2 | | | | | |
| 3 | | | | | |
| 4 | | | | | |
| 5 | | | | | |
| 6 | | | | | |
| 7 | | | | | |
| 8 | | | | | |
| 9 | | | | | |

# Table of Contents

# Chapter 1. General Provisions

## Article 1 (Purpose)

This Policy is the highest level policy document of Nextchip Co., Ltd. (hereinafter, the "Company") and prescribes matters required to security work in the Company.

## Article 2 (Scope of Application)

1. This Policy is applied to everyone who enters the premises of the Company, such as the executives and staff members of the Company and of its affiliates, visitors and customers, and to all information assets of the Company, including tangible and intangible assets and trade secrets owned by the Company.
2. This Policy delineates the following subjects:
   2.1 Definition of the information security of the Company
   2.2 Scope of the information security management system of the Company
   2.3 Direction of the corporate security management that supports the principle and goal of the corporate security
   2.4 Summary of the key policies of the Company and procedures therein
   2.5 Definition of responsibility for security management
   2.6 Other reference materials that are documented and support other policies

## Article 3 (Definitions)

1. The term "Policy" means a principle that prescribe the definition and direction of the information security of the Company as whole.
2. The term "Guideline(s)" means a general rule that delineates the necessity of the policy and the method to realize the policy.
3. The term "Information security" means not only general security activities but also any and all activities that seek a managerial, physical, or technical measure to prevent the leakage, forgery, alteration, or damage of the information which is collected, processed, store, searched, transmitted, or received through an information system or network.
4. The term "Personal information/data" means information relating to a living individual that makes it possible to identify the individual by his/her full name, resident registration number, mark, letter, voice, sound, image, and biometric characteristics etc. (including information which, if not by itself, makes it possible to identify any specific individual if combined with other information) [Article 2 of the Act on Promotion of Information and Communications Network Utilization and Information Protection]
5. The term "Security management state" means the actual condition of the security state of PC, office equipment and office space in each department unit (team, group or office).
6. The term "Information system" means a structured system of hardware and software concerning

collection, processing, storage, search, transmission and receipt, and usage thereof.

7. The term "Auxiliary storage media" means all types of memory device that can be separated from the information and communication network, such as portable hard disk (HDD), USB memory, Flash memory, CD (Compact Disk), DVD (Digital Versatile Disk) or IC chip.
8. The term "Security system" means the type of hardware and software designed to prevent information leakage, forgery, alteration and damage in case of the collection, storage, search, transmission, or receipt of information. CCTV and access-control system designed to protect the facility are also included in this category.
9. The term "Electronic material(s)" means document and printout that is transmitted and received in electronic form through an information processing device, in relation to the Company affairs.
10. The term "Asset" means valuable "information" retained or being handled in the process relating to the policy, technology, production and service of an organization. The term is applied to all subjects of protection that require security, including server, network equipment, security system, supporting device, PC, software, storage media, database(DB), homepage, document file (electronic file), document (hardcopy).
11. The term "Server room" means a place in which the Company's server, PC, switch, exchanger, router, or security system are installed and operated. The access to the server room must be strictly limited to authorized personnel.
12. The term "Access authority" means the authority both to use the information by accessing the information system and to generate, change, read or delete the information.
13. The term "Security accident" means the case of leakage of confidential information or disclosure by either insider or outsider of the Company. In this Policy included are attacks on the information and communication network or the information system related thereto by hacking, computer virus, or malicious code, etc.
14. The term "Confidential information" means a production method, sales method, or other useful technical or managerial asset useful to business activities, of which divulge or leakage to any other person than the persons authorized would cause a serious damage to the Company, as well as civil and criminal responsibility, and the access to which is extremely limited. Confidential information includes trade secret defined by the Unfair Competition Prevention and Trade Secret Protection Act, national core technology defined by the Act on Prevention of Divulgence and Protection of Industrial Technology, and personal information defined by this Policy.
15. The term "Key personnel" means the personnel who, among the executives and staff members, have the authority to access accumulated confidential information and who are subject to the application of personal identification and additional security measures. In this Policy, eternal people who work at the Company based on a contractual relationship are included.
16. The term "Important asset (system)" means, among security level 1 assets, the type of asset that requires legal compliance (such as the Act on Promotion of Information and Communications Network

Utilization and Information Protection, Personal Information Protection Act, and Act on Prevention of Divulgence and Protection of Industrial Technology).

17. The term "Vulnerability" means potential weakness existing in the asset. Although the weakness itself does not cause a danger directly, it can be used by a threat and thus furnish an environment in which a danger or risk can arise.
18. The term "Confidentiality" means a characteristic of practice that keeps information secret and private from unauthorized people, entities, or processes.
19. The term "Integrity" means that information is real and trustworthy as it is protected from unauthorized modification or change, either intentionally or unintentionally.
20. The term "Availability" means a characteristic of practice ensuring that information asset is accessible and usable to authorized entity when requested. In other words, it means that specific assets should be ready for use when needed.
21. The term "Security management system" means a general security operation and management system which includes managerial, physical and technical protection measures to ensure the stability and reliability of the information system. In this Policy, the security management system includes the criteria required in the certification process of security management systems of the certification authorities under ISO27000 (ex.: ISMS. ISO27000, etc.).
22. The term "Security dedicated team/organization" means an organization or a group of people or personnel of which the responsibility, authority, and relationship are defined to perform security activities.
23. The term "Information security manager" means the person or personnel who play a leading role in management of the information system in the Company.

## Article 4 (Duties)

1. The CEO shall establish a security measure to protect the corporate assets and take overall responsibility for security matters.
2. The CEO shall set up a security organization and operate it to perform the security duties efficiently.
3. All employees of the Company and related outside people shall be fully acquainted and comply with this Policy.
4. All employees of the Company and related outside people shall acknowledge and accept that the violation of this Policy will be subject to disciplinary action, or civil and criminal penalties, and that such misconduct can have a negative impact on the Company's business management.
5. All employees of the Company shall follow this Policy for matters not prescribed by other policies, such as HR policy, code of conduct, or disciplinary action policy.

## Article 5 (Maintenance of the Guideline)

1. In consideration of each of the following, the CEO may review the need to change this Policy at least

once a year, regularly and if deemed necessary, the CEO can change the guidelines.

1.1 Change of the corporate business

1.2 Change of the security goal and strategy

1.3 Material change in the structure and manpower of security-related organization(s)

1.4 Material change in the information system

1.5 Serious security accident, and the occurrence of new threat or vulnerability

1.6 Demand of security policy by security-related laws and enterprises that have a contractual relationship with the Company

1.7 Demand of review and revision from other user department(s) or when the CEO deems necessary

2. The Guidelines in this Policy shall be approved by the Security Committee and signed by the CEO, and then shall be published to all employees companywide by means of hardcopy printout or through the electronic bulletin board of the Company.
3. To implement these Guidelines efficiently, each department may establish its own guidelines or operating procedure (manual and guide), separately. Nonetheless, to ensure the consistency with this Guidelines, individual guidelines of the departments shall be reviewed by the security organization before implementation. The security organization shall manage the guidelines of departments as a list, annually.

# Chapter 2. Security Organization

## Article 6 (Structure and Operation of the Security Organization)

1. An executive appointed by the CEO as the information security director shall take the leading role of managing and supervising the security affairs of the Company. The security organization shall be operated under the direction and supervision of the information security director and take charge of various security matters, companywide. The director can select the security organization members by considering the candidates' security education record, qualification license, and other expertise, and shall prepare a method to evaluate their performance.
2. The security organization shall consist of the security committee, information security director, personal information protection director, information security manager, and information security officer.
3. The security committee is the highest level decision-making body concerning the security matters of the Company and shall be convened by the request of the information security director. The security committee shall consist of the information security director and the committee members.
4. The position of information security director shall be taken by the CEO of the company, or an executive authorized by the CEO in a related sector, or an employee whose position is at least the head of a department. In addition to leading the security organization, the information security director shall guide and take overall responsibility for security activities of the Company.

5. The information security managers shall be appointed and authorized by the information security director among the employees whose position is at least the head of a department (team/group/office). The information security managers shall take charge in management of the security organization of the Company.
6. The information security manager of each department (team/group/office) shall be appointed by the head of the department (team/group/office) to which he or she belongs, and shall perform the security tasks of the department (team/group/office) in accordance with the security policy and guidelines of the Company.
7. A person who performs the security task shall maintain and manage the record and printouts that can prove his or her security activity, easily and readily when required.
8. The details of the roles, duties, and job description of the security organization members shall be prescribed in the Personnel Security Management Guidelines.

### Article 7 (Operation of the Security Committee)

1. The security committee serves as the highest security related decision-making body, consisting of the CEO as the chairman and the information security director as the secretary. If another committee, such as the management committee, has the same members as the security committee, a meeting of such another committee can replace the meeting of the security committee.
   1.1 Security activity planning and budget deliberation
   1.2 Review and approval of security policy, guidelines, and procedures
   1.3 Decision of the countermeasures to key security issues
   1.4 Review of the internal inspection result on the performance of the security management system, risk assessment and analysis, and the review of the results.
   1.5 Review and discussion about serious security accidents

## Chapter 3. Personnel Security

### Article 8 (Evaluation of Security Activity)

The information security director shall prepare a management system applicable to the dedicated organization and the members.

### Article 9 (Eligibility Screening of the People Handling Confidential Information)

1. In case of recruitment, the HR department can screen the candidates to confirm their eligibility by way of identification confirmation process, etc.
2. For the personnel who are authorized to access the confidential information of the Company, such as handling key and sensitive information and accessing the information system, the HR department can conduct the eligibility screening by applying the recruitment procedure.
3. General eligibility screening for recruitment shall follow HR-related policy. The details of eligibility

screening over the candidates who may be authorized to handle the confidential information shall be prescribed in the Personnel Security Management Guidelines.

## Article 10 (Execution of the Confidentiality Agreement, Etc.)

1. The HR department shall have all successful applicants sign the security declaration at the time of new employment to protect the key information of the Company, and shall remind them of the content of the declaration when they retire from the Company. If a certain executive or employee is assigned to a job under the defined category of 'national core technology, he or she shall sign a separate security agreement, of which the details shall be prescribed in the Personnel Security Management Guidelines.
2. General matters concerning recruitment and retirement shall follow HR-related policy, and any other matters not prescribed therein shall follow the Personnel Security Management Guidelines.

## Article 11 (Security Management over Outsiders, such as Security in Outsourcing Project, Etc.)

1. When executing a service contract with another company, the contract must specify security requirements to manage and control the information system, network, manpower and working environment, etc. In cases where a contract intends to permit a third party to access the information system and restricted areas, an official agreement that demands compliance with the security policy and key security requirements shall be signed, additionally.
2. If there is a risk of accessing the computer data of the Company by an outsider who provides a service based on a service agreement with the Company, such service agreement shall contain the security requirements to protect the Company's assets and information system.
3. To protect the security of service projects, the head of a department in charge of the service project shall have outside service providers sign and submit the security agreement to the Company, and shall seek a protection measure to prevent the leakage of project outputs.
4. The details of security management over external service projects and outsider security shall be prescribed in the Security Management Guidelines for Outsiders.

## Article 12 (Security Inspection and Internal Investigation)

1. The information security director shall establish a security inspection plan to check the compliance state of the policy and related laws and regulations at least once a year, and report it to the CEO.
2. The scope of the security inspection is as follows, but not limited thereto:
   - 2.1 Implementation of the countermeasure on the results of the risk assessment of the year
   - 2.2 Performance of the overall security management system in all areas of business
   - 2.3 Implementation of certain parts required in the policy or guidelines
   - 2.4 Security areas required by supervisory institutions or another company based on a contractual

relationship with the Company

3. The department (team/group/office) subject to the inspection shall cooperate with the inspection team and obey the improvement requirements given by the inspection team based on the inspection results. Provided, however, the inspection is required in a professional security area, the inspection team must be able to guarantee that its members have professionalism, independence and objectivity.
4. The details of the security inspection and internal investigation shall be prescribed by the Security Inspection Guidelines.

### Article 13 (Security Education)

1. The information security manager shall establish an annual security education plan that lists the date, period, contents, and method of the education, and acquire the approval of the information security director.
2. The information security manager shall provide all members of the Company, the executives and staff members alike, with an education concerning compliance with security policy (personal information protection included), both on a regular basis (once a year) and on need-basis (if necessary).
3. The general matters of security education shall follow the HR-related policy, and any matters not prescribed in the HR-related policy shall be prescribed in the Information Security Education Guidelines.

## Chapter 4. Personal Information Protection

### Article 14 (Principles of Personal Information Protection)

1. The Company shall define the principles of personal information protection and implement them, in order to protect the types of personal information which require management in the course of collection, use, storage, and disposal by the Company.
2. Image information that is under the Company management, and that the Company obtains through CCTV (Closed Circuit Television) or other device which films, collect, and store is also personal information. To protect image information, the Company shall define the protection principles and apply them to the information.
3. The protection measures adopted at the time of collection, retention and use, provision and disposal of personal information are defined as guidelines.
4. If a type of information requires management through the information and communication service for the protection of personal information, the rules of the Act on Promotion of Information and Communications Network Utilization and Information Protection shall be applied. If security control is required in other areas or is required due to the change in the corporate business and work, the Company shall establish a set of Personal Information Protection Management Guidelines, separately and apply the Guidelines to relevant cases.

### Article 15 (Guarantee of the Rights of Information Subject)

1. Unless there is a justifiable reason, the Company shall accept the request of an information subject (customer) to access, correct, delete or suspend his or her own information, and shall record and preserve the details in writing.
2. If the size of the Company exceeds the size specified in personal information protection-related laws and regulations (sales in IT sector, and number of users), the Company shall give notice to the users concerning the Company's collection and use of their personal information, at least once a year.
3. Unless there is an unavoidable reason, in case of the leakage of personal information, the Company shall notify the information subject of the leakage, etc., immediately.
4. Guarantee of the rights of information subjects and other details of personal information protection shall be prescribed in the Personal Information Protection Internal Management Plan Guidelines. If necessary due to the change of corporate business and work, the Company shall establish separate sets of the Personal Information Protection Internal Management Plan Guidelines, and the Personal Information Protection Management Guidelines and apply them to relevant cases.

## Chapter 5. Assets and Risk Management

### Article 16 (Responsibility for Assets)

The managers and the users have their own responsibility over the assets, respectively.

1 The asset managers take overall responsibility for protecting and managing the assets in their possession. The responsibility and role of the asset managers are as follows.

- 1.1 Asset evaluation and determination of the secret grade
- 1.2 Decision of use right and access authority to the asset
- 1.3 Decision and approval of disclosure and taking-out of the asset
- 1.4 Definition of security matters to protect the assets

2 The asset users shall manage and protect their own assets, and realize a proper security measure by analyzing the security matters defined by the asset managers.

3 The asset users shall be defined by the asset managers. The asset users shall practice, diligently, the asset security measures defined and realized by the asset managers and thus protect their acquired assets.

4 The asset users shall not replace, modify, or remove the Company asset, such as hardware and software, at will, and shall obtain the asset manager's approval when they intend to install an unauthorized program, communication device, or secondary storage device thereon.

### Article 17 (Classification of Assets)

1. The list of the Company's assets shall be drafted by the information security manager and be received and managed by the asset management department.
2. The asset list shall be updated at least once a year, and in case of a significant change, the list shall be revised within one (month) after the occurrence of the change.
3. The information security officer shall assign a security grade to each type of asset in consideration of the degree of confidentiality, integrity, and availability, and consider a proper protection measure.
4. The details of asset classification and management shall be prescribed in the Information Asset Security Management Guidelines.

### Article 18 (Asset Risk Assessment)

1. To conduct a risk assessment, the information security manager shall make a list of relevant assets, appoint an officer, and re-review the list at least once a year, regularly.
2. The information security manager shall diagnose the managerial and operational vulnerability, legal (personal security laws) vulnerability, and technical vulnerability as follows, by applying one of the methods provided below.
   2.1 Diagnose the concern and issues, as well as the managerial and operational vulnerability in the operation and management of the information asset subject to the vulnerability diagnosis
   2.2 Check the compliance state of the personal information in the webpages, pursuant to applicable laws (the Personal Information Protection Act), and diagnose the risk of vulnerability on the items that are found unsatisfactory in compliance aspect. Diagnose the vulnerability of the application, as well.
   2.3 Of the assets subject to the vulnerability diagnosis, diagnose the technical vulnerability on the management and operation of the asset defined as 'hardware'.
3. The details of risk assessment on the assets shall be prescribed in the Risk Management Guidelines.

## Chapter 6. Physical Security

### Article 19 (Designation and Management of Restricted Area)

1. The information security director shall designate reserved areas in accordance with the following criteria, to protect the assets in the Company premises.
   1.1 Designate a facility where confidential information is handled and accessed frequently as a restricted area and limit outsider's access thereto.
   1.2 Make sure that people who are not related to the given task will be met at a place designated as common areas.
2. The responsible department shall set up a necessary facility and monitoring system that can control the physical and unauthorized access by an outsider to the inside of the business place. Each entrance

gate in the business place shall be controlled in a manner that can block any unauthorized or irregular entry.

3. CCTV cannot be installed in public places. However, if applicable laws explicitly allow or for the purposes of crime prevention, criminal investigation, facility safety, and fire prevention, CCTV can be installed and operated.
4. The details concerning the management of restricted areas shall be prescribed in the Physical Security Management Guidelines.

## Article 20 (Entry Control)

1. The responsible department shall distinguish entry rights to the restricted areas and apply the entry control system based on fingerprint recognition or the access card, etc.
2. The responsible department shall perform routine checks and monitoring by examining the fingerprint recognition records, and the access card registration and use history, in order to detect any attempts of irregular entry.
3. The information security manager shall perform routine checks and monitoring on the personal entry record to the server room and IDC (cloud) and the equipment entry and taking-out record to find out if any unregistered person has accessed the server room or accessed the equipment, etc.
4. The details concerning the entry control of restricted areas shall be prescribed in the Physical Security Management Guidelines.

## Article 21 (Security of the Communication Device and Other Office Equipment)

1. The information security manager shall establish and implement protection measures to prevent the leakage and disclosure of confidential information through telephones, wired or wireless, in the Company.
2. When introducing an internet telephone system, the information security manager shall make sure that the information and communication network IP address designed for the operation of the information system will not be assigned to the internet telephone system.
3. The details about the communication device and other office equipment shall be prescribed in the Physical Security Management Guidelines.

## Article 22 (Control of Asset Taking-In and Out)

1. In case of asset taking-in and/or out of the business place, the procedure designated based on the confidentiality level of the asset must be observed. Asset taking-in and/or out of the business place by contractors or outside service providers shall be subject to the same rule under the responsibility of a staff member of relevant department (team/group/office).
2. At the time of asset taking-in and/or out, the transaction shall be recorded by way of electric payment,

etc., and the transaction detail shall be submitted to the highest approver of relevant department (team/group/office) or the security organization depending on the asset grade for confirmation.

3. The details about asset taking-in and out shall be prescribed in the Physical Security Management Guidelines.
4. The details about the classification and management of assets shall be prescribed in the Information Asset Security Management Guidelines.
5. The details about the management of auxiliary storage media and documents in the aspect of asset classification shall be prescribed in the Documents and Storage Media Security Guidelines.

### Article 23 (Security Management on Auxiliary Storage Media)

1. The employees of the Company shall comply with the internal policy to prevent important data and information from being leaked through auxiliary storage media or from being infected by malicious code in the media.
2. Other details shall be prescribed in the Information System and Service Security Management Guidelines, and the Documents and Auxiliary Storage Media Management Guidelines.

## Chapter 7. Verification and Access Right Control

### Article 24 (Access Right Control)

1. The information security manager or the security dedicated organization shall make sure that all access to the information system under their responsibility must be through the user verification process, and shall apply each of the following protection measures.
   1.1 Check the access by managers and users to the information system under their responsibility, on a regular basis
   1.2 In case of an internal change, such as new employment, transfer among departments, and retirement, take necessary measures, such as updating or deleting the access right of relevant employees, immediately.
2. With respect to the access rights of the administrators or manager of a system where important information is stacked, the information security manager shall apply stricter management measures, such as checking and changing the password on a regular basis, or checking if the access right has been misused.
3. The information security manager can identify key personnel who handle and operate important information and apply specific protection measures, such as blocking their internet access.
4. Other details shall be prescribed in the Verification and Access Control Guidelines.

### Article 25 (Access Control)

1. The information security manager shall introduce and operate an intrusion prevention system (IPS) or a stricter access control system than the regular security system to protect the key information systems of the Company, and shall apply each of the following protection measures.
   1.1 With respect to important information systems, networks (wireless networks included), application programs and database systems, etc., Apply a pre-defined protection measure and access rules for internet connection or network connection for remote access, and then control or permit the connection. Any unauthorized or irregular connection must be prohibited.
   1.2 Except when the same network address is required for work, Divide the networks by the work type, such as IT service, massive amount of customer information treatment, and general business affairs.
   1.3 Where a guest network is used separately from the internal internet network of the Company, Apply a measure to block the data transmission between the internal internet network and the guest network terminal.
2. Other details shall be prescribed in the Verification and Access Control Guidelines.

## Chapter 8. Application of Encryption

### Article 26 (Management of Information subject to Encryption)

1. The information security manager shall apply encryption to confidential information and personal information, etc. when developing and operating the information systems.
2. The Company assets shall be classified as 'secret', 'classified' or 'general' grades, respectively, depending on the importance and degree of confidentiality. The details of the classification method shall be in accordance with the Asset Security Management Guidelines. The information falls in the category of 'secret' grade shall be deemed as confidential information.

### Article 27 (Management of Confidential Information)

1. In principle, the reading, handling, or distribution of documents shall be restricted depending on the security grade.
2. In the event where the printouts or copies need to be disposed of and the cost exceeds the budget, a method that can ensure the irreparable disposal of the materials must be used, such as shredding by document shredder, incineration, or dissolution. If a piece of confidential information is stored in an auxiliary storage device, the device must be destroyed in such a manner the stored information cannot be ever retrieved.
3. Other details shall be prescribed in the Documents and Auxiliary Storage Media Security Guidelines.

### Article 28 (Encryption Control)

1. In applying encryption to the information system for the purposes of protecting the confidential information of the Company, confidentiality of personal information, integrity, verification and no-reputation, etc., the Company shall prescribe necessary matters and establish guidelines based on relevant laws and regulations, such as the Personal Information Protection Act, and the Act on Promotion of Information and Communications Network Utilization and Information Protection, to prevent security accidents through the employees or developers.
2. In the case of applying the encryption technology to documents, the Company shall examine and select the most suitable program in consideration of the security level, performance level, interchangeability, and the purpose of usage, etc.
   However, if the application of encryption is impossible due to technical limitations and/or system management issues, document encryption may be exempted as an exception based on the approval of the information security manager.
3. The length of an encryption key shall be at least 128 bits for symmetric key encryption, and 2,048 bits for asymmetric key encryption, as recommended by the Korea Internet & Security Agency to prevent damage from brute-force attack (a hacking method that uses all possible passwords and passphrases to find the keys) until 2030
4. For other details, the Company may enact the Encryption Management Guidelines if necessary, depending on the change of corporate business and work.

## Chapter 9. Security Management on the Information System

### Article 29 (Security Management upon the Introduction of Information System)

1. The information security manager or security dedicated organization that retain and manage all information systems shall connect the systems to the network only after eliminating the security vulnerability that has been detected or known.
2. In the case of introducing an information system, the manger shall take each of the following actions, unless the information protection system is the type that has acquired the security certification, domestically or globally.
   2.1 The information security officer shall set up a security plan upon the introduction of the system and acquire the approval of the security manager.
   2.2 When introducing a new information system, the officer shall make sure only authorized software is installed.
   2.3 The manager shall establish the criteria for acceptance approval which reflect the basic security setting for the information system that is being introduced or improved.

2.4 Before accepting the information system, the manager shall perform the conformity test, and document the results for further management.

5. In the case of introducing smart work environment, such as working from home or remote collaboration, the information security manager shall examine potential security concerns and issues first and apply managerial, physical, and technical protection measures, before introducing it.
6. When providing an electronic commerce service, the information security manager shall establish proper measures to prevent data leakage, forgery, fraud, or other types of security accidents. Furthermore, the manager shall check the connection security if the service requires connection with an external system such as payment program. In this case, the requirements of relevant laws, such as the Act on the Consumer Protection in Electronic Commerce, shall be considered.
7. Other details shall be prescribed in the Information System and Security Management Guidelines.

# Chapter 10. Information System and Operation of Security Management

## Article 30 (Log-in Access Control and Security Management)

1. The information security manager shall define the access control function when the developers log-in to the information system.
2. When designing an access control function, the developers shall make sure that it has a security management method about access control by IP, simultaneous connections, detour log-in, automatic log-out, and login record. Also, they shall design the function in such a manner that general user cannot access DB and important files directly without going through an application program.
3. To check and maintain the performance of the information system service, the information security manager shall define the performance checklist items and execute the inspection based on the checklist.
4. In the case of malfunction of the information system service, the information security manager shall analyze the type of trouble, and the trouble-related log and messages, share the details with the system manager, and report to the information security director. In the case of system malfunction due to a security accident, the manager shall cooperate with the security dedicated organization to resolve the problem.
5. The information security manager shall establish a backup and restoration plan for important information systems against the possibility of system malfunction or breakdown, and shall backup important information system and data in accordance with the backup and restoration plan, on a regular basis.
6. Other details shall be prescribed in the Information System and the Service Operation and Management Guidelines.

## Article 31 (Log Control)

1. For all users, the details of their access to the information system and the system usage shall be recorded in the log file. Also, the user access log (user account, IP, time and date, log-in and out time), failure, and printout details shall be recorded.
2. The information security manager shall prescribe the types of log, such as the user access record to the information system, system log, and authority award details, as well as the period and method of record preservation, and shall preserve and manage the information safely.
3. Other details shall be prescribed in the Information System and Service Operation and Management Guidelines.

## Article 32 (Security System Management)

1. The information security manager shall prepare a protective measure to protect the information and communication network.
2. In the event of introducing a security system, the internal procurement procedure and the security of the product should be reviewed. When reviewing the needs of system introduction, the potential issues in the capacity and performance aspects, as well as the interchangeability, stability, and extensibility should be also considered.
3. The information security manager shall establish a guideline for registration, correction and deletion of the security policy of the security system, and operate and manage the system in accordance with the guideline.
4. Other details shall be prescribed in the Information System and Service Security Management Guidelines.

## Article 33 (Program Development and Security Management)

1. The information security manager shall prepare a protective measure to prevent security accidents through the information and communication network and system developers.
2. In the event of introducing a security system, the internal procurement procedure and the security of the product should be reviewed. When reviewing the needs of system introduction, the potential issues in the capacity and performance aspects, as well as the interchangeability, stability, and extensibility should be also considered.
3. The information security manager shall establish a guideline for registration, correction and deletion of the development security policy, and operate and manage the development security system in accordance with the guideline.
4. Other details shall be prescribed in the Information System Development Security Guidelines.

## Article 34 (PC and Server Security)

1. To prevent information violation accidents, when purchasing a server, the internal procurement procedure and the security of the product should be reviewed. When reviewing the needs of system introduction, the potential issues in the capacity and performance aspects, as well as the interchangeability, stability, and extensibility should be also considered.
2. The information security manager shall prescribe any and all security management guidelines and operation responsibility in relation to the usage of terminal units, such as PC and laptops.
3. The information security manager shall provide the PC users with a security measure to prevent unauthorized users' accessing the PC illegally and stealing, forging, altering or damaging the electronic data. The users shall comply with the security measure provided to them.
4. Other details shall be prescribed in the Information System and Service Security Management Guidelines.

# Chapter 11. Response in Emergency Situation

## Article 35 (Security Accident)

1. The information security manager shall distinguish the grade and type of security accidents and respond promptly and accurately, and shall prepare a countermeasure to prevent the recurrence of the accident.
2. In the case of discovering the sign of security accident inside or outside of the Company, the employees of the Company shall report it to the security dedicated organization promptly by using the emergency communication network. Depending on the case, the information security staff of each department may investigate and process the accident reported in cooperation with the information security officer by the order of the information security director and, if necessary, may set up a collaboration system with external experts and/or a company.
3. In the event where a security accident is reported and/or the signs of security accident are detected, if the accident is likely to cause significant damage to the management of the Company, the information security director shall convene the Security Committee meeting, and the accident shall be resolved in accordance with the decision of the management. In this case, if the accident is identified as the leakage of personal information, the Company shall notify the information subject of the issue(notification and report) and take necessary measures to minimize the damage.
4. In the case of Paragraph 3, the Company shall report the result of notification to the information subject and the result of responsive measure to the Korea Internet & Security Agency.
5. The details of security accidents shall be prescribed in the Security Accident Response and Work Continuity Guidelines.

## Article 36 (Emergency Plan)

1. In the case of an occurrence of emergency situation, the information security manager shall set up a responsive measure based on the type of situation and attempt to resume the work, as soon as possible.
2. The information security manager shall establish the work restoration goals and methods, depending on the types of emergency situation, annually. An emergency plan in the IT security aspect can be included, in this case.
3. The information security manager shall set a visual scenario depending on the types of emergency situation and conduct an emergency drill, annually.
4. Other details shall be prescribed in the Security Accident Response and Work Continuity Guidelines.

### Article 37 (IT Accident Restoration Plan)

1. Upon the occurrence of various accidents and emergency situations, the information security manager shall proceed with restoration activities, promptly and systematically. Moreover, the manager shall establish a report system, management department, and management criteria for meticulous follow-up management and put them into practice.
2. Other details shall be prescribed in the Security Accident Response and Work Continuity Guidelines.

## Chapter 12. Maintenance of the Security Management System

### Article 38 (Scope of the Security Management System)

1. To operate the security management system properly, the information security manager shall determine the scope of assets subject to protection, and prepare the following contents for management.

1.1 Security management system, such as the Company's security policy and guidelines

1.2 Physical structure where the asset subject to protection is located and the network structure chart

1.3 Statement of the list of the asset subject to protection

2. Each item in Paragraph 1 can be changed at any time if the change is reviewed in advance at least once a year and the change falls in any of the categories as below:

2.1 Significant change of the physical structure and the network structure of the Company

2.2 Large-scale change in the asset subject to protection

2.3 Significant change in the security requirements of superior laws, supervisory authority, and/or enterprises which have a contractual relationship with the Company

3. The security manager shall create a security management system operation table that includes the state of key security activities (including the subject, role, and work ground, etc.), and review the operation state at least once a year.

### Article 39 (Security Measure Statement)

1. For effective operation of the security management system, the information security manager shall create a statement which shows the security operation state and performance detail based on the security management certification, domestic and international (the "Security Measure Statement"').
2. The security measure statement shall be subject to review for change, at least once a year, regularly; however, in the case of Article 38 Paragraph 2 (Scope of the Security Management System), the statement can be changed at any time.

### Article 40 (Implementation Plan of the Security Management System)

1. The information security manager shall establish a risk reduction implementation plan (the "Security Management System Implementation Plan) concerning the risks detected as a result of the risk assessment prescribed in Article 18 (Risk Assessment of the Asset).
2. The security management system implementation plan may not be established separately, if its contents are included in the security work promotion plan, depending on the implementation time.

### Article 41 (Re-Examination of the Security Management System)

The information security director shall re-examine the internal security management system based on the security inspection results, or audit results, at least once a year and shall improve the problems.

## Addendum

### Article 1 (Effective Date)

This Policy shall take effect on April 22, 2024.

### Article 2 (Superior Laws and Compliance with the Policy)

1. Matters not prescribed in this Policy shall comply with related laws listed below, and contractual requirements with other entities, as well as various internal policies.

1.1 Act on Promotion of Information and Communications Network Utilization and Information Protection

1.2 Personal Information Protection Act

1.3 Act on Prevention of Divulgence and Protection of Industrial Technology

1.4 Unfair Competition Prevention and Trade Secret Protection Act

### Article 3 (Exceptions)

1. Each of the following cases may be accepted as an exception by the approval of the information security director, regardless of whether the issue is dealt with herein.
    1.1 A case where the application of the Policy is impossible due to the change of the technical environment.
    1.2 A case where there is a pressing reason to suspend the application of this Policy due to technical and managerial needs.
    1.3 A force majeure event, such as natural disaster.

## Article 4 (Follow-up Measure)

In the event that the requirements of this Policy are not satisfied due to a specific reason, the Company shall find an improvement method within one (1) year from the effective date.